

SECTION 14: PHYSICAL SECURITY

14.1 General. This section provides facility design guidance for physical security and crime prevention. Established installation security strategies should also be taken into consideration. The purpose of physical security is to make unauthorized access to assets so difficult that an intruder will hesitate to attempt a facility penetration or will, in the course of such efforts, be forced to take actions that will assist in detection or apprehension. Physical security design and construction considerations may include features discussed in Section 15: Force Protection. Please review this section.

14.2 Design Criteria. Guidance for physical security design is provided in MIL-HDBK-1013/1A, "Design Guidelines for Physical Security of Facilities" (reference 14a), OPNAVINST 5530.14C, "Navy Physical Security Manual" (reference 14b), and in using Military Department criteria.

14.3 Passive Security. Facilities should be sited and designed to maximize passive security. Passive security depends largely on staff awareness of the presence of unauthorized persons. This concept includes the use of security zoning within a facility. Specific using Military Department criteria shall be followed. The following are recommended considerations:

14.3.1 Access Control. Proper design permits staff to control specific areas of responsibility, thereby reducing or eliminating the opportunity for undesirable behavior within a designated area by restricting access to only those authorized personnel having legitimate reasons for access. Consideration should be given to vehicular and pedestrian access routes, parking layouts, landscaping, lighting, and location and design of department reception areas and other operational functions to assist in controlling access.

14.3.2 Proximity Placement. Planning and design should take into consideration collocating, if feasible, departments of similar sensitivity and access requirements along with the design of parking layouts, entrances, and personnel traffic patterns to maximize the effectiveness of an access control system.

14.3.3 Visibility. Locations of reception desks should afford unrestricted visibility of entrances, thereby establishing entry control points. Traffic patterns must bring traffic to these control points to ensure effective 24-hour staff control.

14.4 Physical Construction. Physical construction should be designed to prevent unauthorized access to high value assets, i.e., to resist break-in to security cages, pharmacies, vaults, storerooms, mail rooms, etc. Mail rooms should be located at the perimeters of facilities.

14.5 Electronic Security Systems.

14.5.1 Systems Considerations. Electronic security systems, including Intrusion Detection Systems (IDS), duress alarms, electronic access control systems and Closed Circuit Television (CCTV) systems, shall be provided for facilities when required by the using Military Department. Multiple electronic security systems may be integrated to provide an overall facility security system. A staff identification card system with multiple levels of access control may be provided. Package inspection devices may

also be considered for mail rooms. See Section 11: Communications Systems for information on electronic security systems.

14.5.2 Systems Design. Construction documents for electronic security systems shall identify sensor locations and include floor plans, schematics, riser diagrams, security equipment schedules and typical details. Floor plans shall locate all monitoring and control equipment. Security equipment schedules shall include room and door numbers, sensors, alarm control panels, switches and access control devices. Electronic security systems shall be provided with uninterruptible power sources, dedicated electrical service panels, interfaces with installation security systems, and local and remote alarms, as required by the using Military Department.

14.6 Keys and Locks. The master key and lock plan for a facility shall provide multiple levels of entry control. A master key system shall be provided for all areas with the following exceptions. Separate keying systems are required for pharmacies. Separate keying systems should also be considered for medical supply storage areas or facilities; food service facilities; exchange service facilities; mail rooms; mechanical, electrical and communications equipment rooms; and housekeeping and janitorial rooms.

14.7 External Security. External security protection should be provided primarily by proper illumination and by parking layouts that minimize staff walking distances to entrances. Where possible, parking areas should be located so that they can be viewed entirely from entry control points within a facility such as the emergency department or other primary entrances. Site landscaping adjacent to a facility should consider physical security concerns, i.e., possible concealment of intruders, etc. For those facilities that are not on installations or that are in remote locations on installations, fencing should be considered at the site perimeter. The entire perimeter should be well lighted with minimal use of shrubs and trees for possible concealment of intruders.

14.8 Levels of Security Protection. The essential requirement is to provide an appropriate level of security protection for personnel and property. The objective is to decrease the opportunity for security problems to develop. The following levels of security protection are defined according to operational mission:

14.8.1 Medical Facilities Excluding Hospitals. In addition to the preceding security considerations:

14.8.1.1 Intrusion Detection Systems (IDS). Exterior doors and operable windows shall be provided with IDS sensors with alarms monitored at the installation security station and at other locations if required by the using Military Department.

14.8.1.2 Other Considerations. Other basic security devices with local and remote alarms shall be included for narcotics lockers, precious metals safes, and medical supply storage areas or facilities.

14.8.2 Hospitals. In addition to the above, security shall be further enhanced by:

14.8.2.1 Traffic Patterns. Traffic patterns that can be controlled with a minimum of entry control points during nighttime hours in a facility staffed 24 hours a day. In hospitals where the emergency department entrance is the only staffed entrance during these hours, visitors should enter within direct control of the emergency department reception desk. Other entrances such as those for dental or other clinics shall be locked

after normal operating hours. IDS sensors and CCTV systems should be installed at these entrances.

14.8.2.2 Remote Locking. Remote, electrically operated locks that can be controlled from a central point such as the emergency department reception desk or a hospital command and control center. This system establishes the emergency department reception desk or the command and control center as the hospital Central Security Operations Point after daytime hours. Such locks must be released automatically, when fire and smoke alarms are activated, for doors required for emergency egress.

14.8.2.3 Intrusion Detection Systems (IDS). IDS planned and designed to meet the security requirements of the location and the using Military Department directives.

14.8.2.4 Closed Circuit Television (CCTV) Systems. CCTV systems for areas as specified by the using Military Department.

14.8.2.5 Card Access Systems. Card access systems for exterior doors and sensitive areas such as computer rooms, pharmacies, and other areas as specified by the using Military Department.

14.9 Special Considerations for Security Sensitive Areas/Rooms. Sensitive areas/rooms shall be designed to store valuable assets, i.e., funds, narcotics, dangerous drugs, and controlled substances/materials. The most cost-effective method of providing adequate security for these assets shall be selected.

14.9.1 Funds Storerooms. Design considerations shall include the possible use of roll-up shutters, special wall construction, special door construction and hardware, prevention of access from ceiling spaces, IDS and duress alarms, security glazing for service windows, nighttime security lighting and special key control. Security features will be determined by the using Military Department based on the dollar amount of funds to be stored.

14.9.2 Safes. Drugs classified as Schedule I or II controlled substances under the Controlled Substance Act of 1970 must be stored in safes or vaults. Drugs classified as Schedule III through V may also be stored in safes or vaults as deemed appropriate by the using Military Department. Safes or steel security containers, weighing less than 750 pounds, shall be bolted or cemented to floors or walls in such a way that they cannot be readily removed. Safes and steel security containers, if necessary due to the quantities and types of controlled substances/materials to be stored, shall be equipped with IDS.

14.9.3 Vaults. Features to be considered for vault storage areas are outlined in MIL-HDBK-1013/1A (reference 14a) and using Military Department directives.

14.9.3.1 Vault Construction.

a) Walls, floors and ceilings of vaults must be constructed of at least eight inches of reinforced concrete, or other substantial masonry, reinforced vertically and horizontally with 15 millimeter (1/2-inch) steel rods tied together at 150 millimeters (6-inches) on center, or the structural equivalent to such reinforced walls, floors and ceilings.

b) Vault door and frame units must meet the following requirements for resisting unauthorized entry: 30 minutes against surreptitious entry, 10 minutes against forced entry, 20 work hours against

lock manipulation, and 20 work hours against radiological techniques. Vault doors must be equipped with contact switches.

c) Additionally, vaults must be equipped with one of the following: complete electrical lacing of walls, floors and ceilings; sensitive ultrasonic or infrared sensors within the vaults; sensitive sound accumulator systems; or such other systems designed to detect unauthorized entry as may be required by the using Military Department. Vault alarm systems shall transmit a signal directly to the Central Security Operations Point and/or the installation security station, i.e., a location that is staffed 24-hours a day.

14.9.3.2 Day Gates. Vaults that must remain open during normal operating hours shall be provided with self-closing and self-locking day gates complying with using Military Department requirements.

14.9.4 Pharmacies. Walls, floors and ceilings of pharmacies shall provide resistance to forced or surreptitious entry and, where necessary, shall be reinforced. Doors and windows shall be kept to a minimum and doors shall be keyed separately from the master key system. IDS sensors shall be installed at all doors and windows including windows opening to corridors. Walls surrounding pharmacies shall be constructed in accordance with MIL-HDBK-1013/1A (reference 14a). As a minimum, perimeter walls shall be full height from floor slab to structure above.

14.9.4.1 Doors. Doors shall be provided with security hinges and shall be locked with security locksets. Doors may be lightweight, covered with 9 to 12 gauge steel security mesh or 16 gauge sheet steel fastened with smooth-headed bolts and nuts peened in place. Other considerations include "peep holes," a cipher lock or card access system for the main staff entrance door, double locking locksets with 1-inch throws, warning signs stating doors must remain unlocked during normal operating hours (for fire egress), and warning signs stating "Controlled Area."

14.9.4.2 Windows. Provisions such as roll-up shutters, shall be made for securing all service windows after normal operating hours. Frames holding roll-up shutters and security screens or bars must be securely fastened with smooth-headed bolts with nuts peened in place.

14.9.4.3 Heating and Ventilation Ducts. Duct terminals and connecting points must be in exposed locations where they may be readily observed to detect tampering. Openings of eight inches or larger must be protected with 9 to 12 gauge steel security mesh. The mesh will either be welded to the duct or secured with smooth-headed bolts with nuts peened in place.

14.9.5 Medical Supply Storage Areas or Facilities. In addition to the criteria provided for Pharmacies above, high value, critical and pilferable resources stored in this type of storage area or facility shall be enclosed within two or more time-delay barriers, i.e., fences, security cages, building walls, vaults or locked doors. For specific requirements, see MIL-HDBK-1013/1A (reference 14a) and using Military Department directives.

14.9.6 Other Security Sensitive Areas/Rooms. Other activities or locations may be identified by the using Military Department as security sensitive. These areas/rooms must minimize the security risk for these activities or locations.

REFERENCES

- 14a. MIL-HDBK-1013/1A, "Design Guidelines for Physical Security of Facilities."
(http://www.efdlant.navfac.navy.mil/Lantops_15/ENGR_index.htm)
- 14b. OPNAVINST 5530.14C, "Navy Physical Security Manual."